

## GUIDANCE

# Responding to a Cardholder Data Breach

This guide is intended to help merchants and service providers with incident response preparation. This guide also describes how and when a Payment Card Industry Forensic Investigator (PFI) should be engaged to assist.

Only PFIs listed on the [PCI SSC website](#) are approved by PCI SSC to provide forensic investigation services in the event of a payment card breach.



## PREPARATION FOR DATA BREACH MANAGEMENT

### Implement an Incident Response Plan

Your organization should ensure that effective incident-management controls are in place. PCI DSS Requirement 12.10 is essential in this effort. It requires entities to “Implement an incident response plan. Be prepared to respond immediately to a system breach.”

Guidance in this PCI DSS requirement notes that this should be a “thorough incident response plan that is properly disseminated, read, and understood by the parties responsible.” It should include proper testing exercises at least annually to ensure the process works as designed and to mitigate any missed steps to limit exposure.

### Limit Data Exposure

Knowing how to limit data exposure and minimize data loss while preserving evidence is essential. For example, make sure you know how to isolate systems without simply powering them off. Turning systems off may make the investigation more difficult and result in lost evidence or data. For more information about evidence preservation, see the section titled “Working With Your PFI” on page 3.

### Understand Notification Requirements

Be prepared to alert necessary parties immediately. Having a plan and ensuring current and accurate contact information for each party must be validated regularly. This plan will include payment card brands, acquirers (merchant banks), and any other entities that may require notification, whether by contract or law.

### Manage Third-Party Contracts

Make sure that all contracts with third-party service providers, hosting providers, integrators/resellers, and other relevant parties address incident-response management sufficiently. Contracts should include specific provisions on how evidence from those environments will be accessed



and reviewed, such as allowing your PFI access to the environments. Contracts should include provisions to require the third party's cooperation and allow a PFI to broaden the investigative scope to the third party if the third party is found to be the source of (or contributed to) an event that impacted cardholder data security.

## IDENTIFY A PFI

Some PFIs offer their services on retainer. You can consider such an agreement so that you have a PFI company ready to call when you need it.

You may also consider identifying and talking to several PFI companies qualified to serve in your region in case one is unavailable when you need it or if you have specific needs that can be served only by certain PFIs.

Keep in mind that all PFIs are required to meet strict independence requirements to prevent conflicts of interest. Therefore, a company you use for other PCI services (for example, QSA services) cannot also be used for your PFI investigation.



## ENGAGING A PFI

### When to Engage a PFI

If a cardholder data breach has occurred or is suspected, the payment brands may require an independent forensic investigation to be completed by a PFI listed on the PCI SSC website.

Since acquirers and the payment brands each have their own rules and thresholds about when a PFI must be engaged, contact the acquirers or payment brands to make this determination. For payment brand contact information, see FAQ 1142 on the PCI SSC website.



### What to Expect From Your PFI

Whether your acquirer notified you of a suspected breach or you detected it and contacted the acquirer yourself, you may be required to engage the services of a PFI. Understanding the role and how to engage a PFI is vital for successful incident management. Keep in mind the following considerations when selecting a PFI:

- PFIs are required to be independent of the entity under investigation. When choosing a PFI, make sure your company has no other relationships with the PFI that could create a conflict of interest or violate this independence. For example, if your Qualified Security Assessor (QSA) is also a PFI, it cannot perform your investigation. Other forensic investigators (i.e., non-PFIs) or any other outside consultants (legal counsel, technical advisors, etc.) hired by or representing your company must not interfere with the PFI's investigation. The PFI must perform its own investigation and cannot accept influence, direction, or reports from outside consultants. While it is common for the payment brands to ask the merchant to report details of the incident to the PFI, this report is intended only to provide the PFI with information to help assess what has already been completed, and is not intended to be part of the PFI's report.
- PFIs provide a 24x7x365 first-level phone and incident response for the regions in which they are qualified to operate, and must be able to initiate an investigation within five business days of signing an agreement. Choose a PFI listed for the region(s) in which you think the breach has occurred.
- The investigation will be supervised by a Lead Investigator and may be conducted remotely or onsite. If the investigation is remote, the PFI will give detailed instructions about how to handle and transfer evidence securely for examination in the PFI's laboratory environment.
- The PFI looks at your environment from a different perspective than your QSA, Internal Security Assessor (ISA), or your own self-assessment efforts. As such, what may have been

previously defined as the PCI DSS or cardholder data environment (CDE) scope may need to be extended for the PFI investigation to find the root cause of the intrusion. The PFI will determine the full scope of the investigation and the relevant sources of evidence.

- The PFI will perform extensive investigation and reporting to understand what happened. You can expect to receive a PFI Preliminary Report and a Final PFI Report (both on PCI SSC's mandatory reporting templates). These reports will also be provided to your acquirer (if you have such a contract) and the affected payment brands.
- While the PFI will not perform a full PCI DSS assessment, the PFI will report about whether deficiencies in compliance with PCI DSS requirements were observed during his investigation. This does not constitute a full PCI DSS assessment, nor does a lack of findings imply PCI DSS compliance.
- If a PIN data compromise is suspected, the PFI will also perform a PIN-security and key-management investigation. A PCI PIN security assessment may also be necessary.

## What Support Will a PFI Provide?

Based on its findings, the PFI will make recommendations about how your organization should prioritize containment and secure account data while preserving the integrity of evidence. These recommendations are intended to complement your internal incident response plan. It is important for the recommendations to be implemented as soon as possible to help reduce the risk of further data loss or further compromise.

Because the PFI is required to validate containment prior to issuing their final report, they may make recommendations during the investigation process. It is important to begin implementing the PFI's recommendations promptly rather than waiting until the final report is issued.

## Working With Your PFI

To complete a thorough and effective investigation, the PFI will require access to data, facilities, and people. This may also include access to third-party service providers who store, process, or transmit cardholder data on your behalf or who can otherwise affect the security of the cardholder data environment (for example, website hosting providers and web application vendors).

When a breach occurs or is suspected, it is critical to preserve the evidence. It may be tempting to reboot devices, clear up log files, update security patches, remove suspect software, and generally try to recover as quickly as possible. However, careful preservation of evidence is vital both in isolating the root cause of the breach and in identifying the perpetrators. Because digital evidence is easily contaminated, maintaining a strict chain of custody is crucial to achieving useful investigation results.

## Evidence Preservation

1. Unless otherwise instructed by your PFI, do not access or alter compromised system(s) (that is, do not log onto the compromised system(s) or change passwords, do not log in as ROOT, admin, etc.). To avoid losing critical data, it is highly recommended that the compromised system(s) not be used.
2. Unless otherwise instructed by your PFI, do not turn the compromised system(s) off. Instead, isolate compromised systems(s) from the network (for example, unplug network cable or revoke/disable wireless access).
3. Preserve all evidence and logs, such as original evidence, security events, web, database, firewall, and so on. Make sure the integrity of the evidence is not impacted by any tools used in the collection and analysis process.
4. Document all actions taken, including dates, times, and individuals involved.

## Facilities

The PFI will determine what facilities must be visited or reviewed. It is important that the compromised entity understands access to the facilities may provide vital insight into what happened.

As mentioned earlier, this access may be complicated when facilities include third-party service providers. Proactive work with these parties is important to ensure that a PFI has the needed access to the third-party site, whether physical or remote, to conduct the investigation.

## People



Ensure that appropriate employees – for example, CTOs, network administrators, and IT security managers – are available to meet with the PFI in a timely manner. Employees should be open, honest, and understand the role of the PFI. The PFI is not there to assign blame. They want to ascertain what happened and help the organization recover quickly.

## Feedback





PFI are required to provide their customers with a feedback form (or refer them to the form available on the PCI SSC website) which is submitted directly to PCI SSC. PFI are subject to a quality-assurance program operated by PCI SSC, and all feedback is encouraged as input to this process.

## STAKEHOLDER ROLES AND RESPONSIBILITIES

All participants in the payment system play a major role in upholding the highest information security standards and protecting cardholder data, wherever it resides. Each participant also has a role in a data breach event.

Role	Responsibility
 <p><b>ACQUIRING BANK</b></p> <p>Also known as merchant bank. A financial institution that establishes accounts for merchants, allowing the merchants the ability to accept payment cards.</p> <p>Has contractual agreement with the merchant.</p> <p>Ensures a merchant is PCI DSS compliant.</p> <p>Establishes the compliance validation requirements for their merchants, including direct receipt of any validation documentation from the merchant.</p>	<ul style="list-style-type: none"> <li>• Can require the PFI investigation.</li> <li>• Ensures the merchant engages the PFI.</li> <li>• Establishes investigation status calls (can be irregular or regular).</li> <li>• Participates on investigation status calls.</li> </ul> <ul style="list-style-type: none"> <li>• Takes roll call of all participants.</li> <li>• Manages meeting agenda.</li> <li>• Restates next steps.</li> <li>• Participates on the final forensic call.</li> <li>• Depending on the results of the final forensic report, provides at-risk accounts for card brands.</li> </ul>
 <p><b>CARD BRANDS</b></p> <p>American Express, Discover, JCB, Mastercard, Visa</p> <p>Acts as a merchant bank (American Express, Discover) or an entity (JCB, Mastercard, Visa) who works with merchant banks to ensure merchants and service providers protect cardholder data according to the Payment Card Industry Data Security Standard (PCI DSS).</p> <p>Each manages its own PCI DSS compliance program regarding merchants, service providers, etc.</p>	<ul style="list-style-type: none"> <li>• Can require the PFI investigation.</li> <li>• Participates on investigation status calls.</li> </ul> <ul style="list-style-type: none"> <li>• Participates on the final forensic call.</li> <li>• Provides feedback, requests clarifications, and may require revisions to final report.</li> </ul>

(CONTINUED ON NEXT PAGE)

Role	Responsibility
 <p><b>INDEPENDENT SALES ORGANIZATION (ISO)</b></p> <p>A third-party agent that partners with merchant banks to establish and manage merchant accounts on behalf of the merchant banks. ISOs may also be referred to as merchant service providers or processor when they offer financial transaction processing services.</p> <p>May also manage PCI DSS compliance programs on behalf of the merchant bank and establish the compliance validation requirements for their Level 4 merchants.</p>	<ul style="list-style-type: none"> <li>• A processor acting on behalf of a merchant bank has the same responsibilities of the merchant bank as it pertains to a forensic investigation. However, the merchant bank must also participate on investigation status calls and the final forensic call.</li> <li>• Can require the PFI investigation.</li> <li>• Ensures the merchant engages the PFI.</li> <li>• Establishes investigation status calls (can be irregular or regular).</li> <li>• Participates on investigation status calls.</li> <li>• Takes roll call of all participants.</li> <li>• Manages meeting agenda.</li> <li>• Restates next steps.</li> <li>• Participates on the final forensic call.</li> <li>• Depending on the results of the final forensic report, provides at-risk accounts for card brands.</li> </ul>
 <p><b>MERCHANT</b></p> <p>A seller of goods or services that agrees to accept payment cards.</p>	<ul style="list-style-type: none"> <li>• Can initiate the PFI investigation.</li> <li>• Engages with PFI.</li> <li>• Provides access and documentation to PFI of the cardholder data environment.</li> <li>• Participates on investigation status calls.</li> <li>• Provide documentation or clarification to brands' request for information.</li> <li>• Participates on the final forensic call.</li> <li>• Provide feedback on the PFI to the PCI SSC.</li> </ul>
 <p><b>PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL (PCI SSC)</b></p> <p>An independent organization that maintains responsibility for management of payment card industry security standards including the PCI Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS).</p> <p>Manages the PCI Forensic Investigator (PFI) program.</p>	<ul style="list-style-type: none"> <li>• Has oversight of the PFI program.</li> <li>• Answers questions regarding the PFI Program Guide, PFI Qualification Requirements, PFI Preliminary Incident Response Report Template, PFI PIN Security Requirements Report Template, and the Final PFI Report Template.</li> <li>• Does not participate on investigation status calls or final forensic calls.</li> <li>• Does not receive, review, or have access to forensic reports.</li> <li>• Does not manage compliance programs.</li> </ul>
 <p><b>THIRD-PARTY AGENT/SERVICE PROVIDER</b></p> <p>May offer processing services, technical support services (including but not limited to network support, Point-of-Sale application support), e-commerce hosting services, call center services, etc.</p>	<ul style="list-style-type: none"> <li>• If required, provide documentation or artifacts to the PFI.</li> <li>• If necessary, participates on investigation status calls.</li> <li>• Provides documentation or clarification to brands' request for information.</li> <li>• If necessary, participates on the final forensic call.</li> </ul>